

CLAIMS

What is claimed is:

- 1 1. A method of scanning a requested file for a computer malware
2 comprising the steps of:
3 receiving a request to transfer a file from computer malware scanning
4 software;
5 receiving a request from the computer malware scanning software for
6 data comprising a randomly accessed portion of the requested file; and
7 transferring the requested portion of the file and supplying the requested
8 data to the computer malware scanning software to fulfill the request for data
9 comprising a portion of the requested file.
- 1 2. The method of claim 1, wherein the request to transfer the file from the
2 computer malware scanning software comprises a request to transfer the file
3 from an external system.
- 1 3. The method of claim 2, wherein the external system is communicatively
2 connected via a network.
- 1 4. The method of claim 3, wherein the network comprises the Internet.

NAI-03.011.01

1 5. The method of claim 4, wherein the step of transferring the requested
2 portion of the file comprises the step of:

3 initiating a session with the external system to obtain the requested
4 portion of the file.

1 6. The method of claim 5, wherein the session is a hypertext transfer
2 protocol session.

1 7. The method of claim 6, wherein the hypertext transfer protocol session
2 uses a byte range technique.

1 8. The method of claim 7, further comprising the steps of:
2 determining that the requested portion of the requested file cannot be
3 transferred; and
4 transferring the entire requested file and supplying the requested data to
5 the computer malware scanning software to fulfill the request for data
6 comprising a portion of the requested file.

1 9. The method of claim 8, wherein the requested portion of the requested
2 file cannot be transferred because the requested portion of the requested file
3 cannot be randomly accessed.

1 10. The method of claim 9, wherein an indication that the requested portion
2 of the requested file cannot be randomly accessed comprises an error
3 indication or a transfer of the entire requested file.

1 11. The method of claim 7, further comprising the steps of:
2 tracking information associated with each transfer of a requested portion
3 of the file; and
4 determining that information associated with the file has changed.

1 12. The method of claim 11, wherein the information associated with the
2 file comprises hypertext transfer protocol entity tags or last modified timestamp
3 information.

1 13. The method of claim 12, further comprising the step of:
2 restarting the requests from the computer malware scanning software for
3 data.

1 14. The method of claim 13, further comprising the step of:

2 transferring the entire requested file.

1 15. The method of claim 1, further comprising the step of:

2 performing the steps of claim 1 in response to a request from a user
3 system for the file.

1 16. The method of claim 15, further comprising the steps of:

2 scanning at the computer malware scanning software the data
3 comprising a portion of the requested file to determine if the file includes a
4 computer malware; and

5 delivering the file to the user system in response to determining that the
6 file does not include a computer malware.

1 17. The method of claim 16, wherein the step of delivering the file to the
2 user system comprises the steps of:

3 determining whether the entire file has been transferred;

4 starting delivery of the file to the user system even if the entire file has
5 not been transferred; and

6 transferring those portions of the file that have not been transferred and
7 delivering those portions of the file once they have been transferred.

1 18. The method of claim 17, wherein the step of transferring those portions
2 of the file that have not been transferred comprises the step of:

3 initiating a session with the external system to obtain those portions of
4 the file that have not been transferred.

1 19. The method of claim 18, wherein the session is a hypertext transfer
2 protocol session.

1 20. The method of claim 19, wherein the hypertext transfer protocol session
2 uses a byte range technique.

1 21. A system of scanning a requested file for a computer malware virus
2 comprising:

3 a processor operable to execute computer program instructions;

4 a memory operable to store computer program instructions executable
5 by the processor; and

6 computer program instructions stored in the memory and executable to
7 perform the steps of:
8 receiving a request to transfer a file from computer malware scanning
9 software;
10 receiving a request from the computer malware scanning software for
11 data comprising a randomly accessed portion of the requested file; and
12 transferring the requested portion of the file and supplying the requested
13 data to the computer malware scanning software to fulfill the request for data
14 comprising a portion of the requested file.

1 22. The system of claim 21, wherein the request to transfer the file from the
2 computer malware scanning software comprises a request to transfer the file
3 from an external system.

1 23. The system of claim 22, wherein the external system is
2 communicatively connected via a network.

1 24. The system of claim 23, wherein the network comprises the Internet.

1 25. The system of claim 24, wherein the step of transferring the requested
2 portion of the file comprises the step of:
3 initiating a session with the external system to obtain the requested
4 portion of the file.

1 26. The system of claim 25, wherein the session is a hypertext transfer
2 protocol session.

1 27. The system of claim 26, wherein the hypertext transfer protocol session
2 uses a byte range technique.

1 28. The system of claim 27, further comprising the steps of:
2 determining that the requested portion of the requested file cannot be
3 transferred; and
4 transferring the entire requested file and supplying the requested data to
5 the computer malware scanning software to fulfill the request for data
6 comprising a portion of the requested file.

1 29. The system of claim 28, wherein the requested portion of the requested
2 file cannot be transferred because the requested portion of the requested file
3 cannot be randomly accessed.

1 30. The system of claim 29, wherein an indication that the requested portion
2 of the requested file cannot be randomly accessed comprises an error
3 indication or a transfer of the entire requested file.

1 31. The system of claim 27, further comprising the steps of:
2 tracking information associated with each transfer of a requested portion
3 of the file; and
4 determining that information associated with the file has changed.

1 32. The system of claim 31, wherein the information associated with the file
2 comprises hypertext transfer protocol entity tags or last modified timestamp
3 information.

1 33. The system of claim 32, further comprising the step of:
2 restarting the requests from the computer malware scanning software for
3 data.

1 34. The system of claim 33, further comprising the step of:

2 transferring the entire requested file.

1 35. The system of claim 21, further comprising the step of:

2 performing the steps of claim 1 in response to a request from a user
3 system for the file.

1 36. The system of claim 35, further comprising the steps of:

2 scanning at the computer malware scanning software the data
3 comprising a portion of the requested file to determine if the file includes a
4 computer malware; and

5 delivering the file to the user system in response to determining that the
6 file does not include a computer malware.

1 37. The system of claim 36, wherein the step of delivering the file to the
2 user system comprises the steps of:

3 determining whether the entire file has been transferred;

4 starting delivery of the file to the user system even if the entire file has
5 not been transferred; and

6 transferring those portions of the file that have not been transferred and
7 delivering those portions of the file once they have been transferred.

1 38. The system of claim 37, wherein the step of transferring those portions
2 of the file that have not been transferred comprises the step of:

3 initiating a session with the external system to obtain those portions of
4 the file that have not been transferred.

1 39. The system of claim 38, wherein the session is a hypertext transfer
2 protocol session.

1 40. The system of claim 39, wherein the hypertext transfer protocol session
2 uses a byte range technique.

1 41. A computer program product of scanning a requested file for a computer
2 malware comprising:

3 a computer readable medium;

4 computer program instructions, recorded on the computer readable

5 medium, executable by a processor, for performing the steps of

6 receiving a request to transfer a file from computer malware scanning
7 software;
8 receiving a request from the computer malware scanning software for
9 data comprising a randomly accessed portion of the requested file; and
10 transferring the requested portion of the file and supplying the requested
11 data to the computer malware scanning software to fulfill the request for data
12 comprising a portion of the requested file.

1 42. The computer program product of claim 41, wherein the request to
2 transfer the file from the computer malware scanning software comprises a
3 request to transfer the file from an external system.

1 43. The computer program product of claim 42, wherein the external system
2 is communicatively connected via a network.

1 44. The computer program product of claim 43, wherein the network
2 comprises the Internet.

1 45. The computer program product of claim 44, wherein the step of
2 transferring the requested portion of the file comprises the step of:

3 initiating a session with the external system to obtain the requested
4 portion of the file.

1 46. The computer program product of claim 45, wherein the session is a
2 hypertext transfer protocol session.

1 47. The computer program product of claim 46, wherein the hypertext
2 transfer protocol session uses a byte range technique.

1 48. The computer program product of claim 47, further comprising the steps
2 of:

3 determining that the requested portion of the requested file cannot be
4 transferred; and

5 transferring the entire requested file and supplying the requested data to
6 the computer malware scanning software to fulfill the request for data
7 comprising a portion of the requested file.

1 49. The computer program product of claim 48, wherein the requested
2 portion of the requested file cannot be transferred because the requested
3 portion of the requested file cannot be randomly accessed.

1 50. The computer program product of claim 49, wherein an indication that
2 the requested portion of the requested file cannot be randomly accessed
3 comprises an error indication or a transfer of the entire requested file.

1 51. The computer program product of claim 47, further comprising the steps
2 of:
3 tracking information associated with each transfer of a requested portion
4 of the file; and
5 determining that information associated with the file has changed.

1 52. The computer program product of claim 51, wherein the information
2 associated with the file comprises hypertext transfer protocol entity tags or last
3 modified timestamp information.

1 53. The computer program product of claim 52, further comprising the step
2 of:
3 restarting the requests from the computer malware scanning software for
4 data.

1 54. The computer program product of claim 53, further comprising the step
2 of:
3 transferring the entire requested file.

1 55. The computer program product of claim 41, further comprising the step
2 of:
3 performing the steps of claim 1 in response to a request from a user
4 system for the file.

1 56. The computer program product of claim 55, further comprising the steps
2 of:
3 scanning at the computer malware scanning software the data
4 comprising a portion of the requested file to determine if the file includes a
5 computer malware; and
6 delivering the file to the user system in response to determining that the
7 file does not include a computer malware.

1 57. The computer program product of claim 56, wherein the step of
2 delivering the file to the user system comprises the steps of:
3 determining whether the entire file has been transferred;

4 starting delivery of the file to the user system even if the entire file has
5 not been transferred; and
6 transferring those portions of the file that have not been transferred and
7 delivering those portions of the file once they have been transferred.

1 58. The computer program product of claim 57, wherein the step of
2 transferring those portions of the file that have not been transferred comprises
3 the step of:

4 initiating a session with the external system to obtain those portions of
5 the file that have not been transferred.

1 59. The computer program product of claim 58, wherein the session is a
2 hypertext transfer protocol session.

1 60. The computer program product of claim 59, wherein the hypertext
2 transfer protocol session uses a byte range technique.